

This is Cyber:
1 + 3 Challenges for the Application of
International Humanitarian Law in Cyberspace

Kubo Mačák

Exeter Centre for International Law

Working Paper Series

2019/2

Exeter Centre for International Law

The Exeter Centre for International Law builds on a long and distinguished tradition of international legal scholarship at Exeter Law School. The Centre's mission is to provide an intellectual environment for the study and development of international law and to stimulate discussion and collaboration in response to the most pressing challenges facing the international community. As part of this mission, the Centre publishes the present Working Paper Series.

Centre Director: Aurel Sari
General Editor: Michael N. Schmitt
Editor in Chief: Kubo Mačák

Exeter Centre for International Law
Exeter Law School, Amory Building
Rennes Drive, Exeter, EX4 4RJ, United Kingdom

 <http://www.exeter.ac.uk/ecil>
 [@ExeterCIL](https://twitter.com/ExeterCIL)

© All rights reserved. No part of this paper may be reproduced in any form without the permission of the author.

Cite as Kubo Mačák, "This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace", ECIL Working Paper 2019/2.

*Kubo Mačák**

Introduction

This year we commemorated ten years since the death of the American writer David Foster Wallace. I am not sure that he wrote or even thought much about cyber warfare and certainly not about the legal connotations of malicious conduct in cyberspace. In fact, it is probably fair to say that he held some strange combination of detached admiration and bemused disdain for cyber experts—or, in his exact words, “skinny, carbuncular, semi-autistic Computer Nerds” who, when your computer stops working, look at you condescendingly and perform “the two occult keystrokes that unfreeze your screen”.¹

And yet, I think that Wallace’s thinking is a good point at which to begin this lecture on the contemporary challenges that cyber operations pose for international law. In 2005, Wallace delivered his famous commencement speech to the graduating class at Kenyon College in Ohio in the US.² In it, he shared this amusing little parable with the students:

There are these two young fish swimming along and they happen to meet an older fish swimming the other way, who nods at them and says “Morning, boys. How’s the water?” And the two young fish swim on for a bit, and then eventually one of them looks over at the other and goes “What the hell is water?”³

Later on in the speech, Wallace explained what he had meant by the parable:

The point of the fish story is ... that the most obvious, ubiquitous, important realities are often the ones that are hardest to see and talk about.⁴

This was a commencement speech and Wallace was speaking about the value of education. But his observation that invisible realities are often the crucial ones extends beyond the scope of his speech. In fact, I believe it to offer a very fitting metaphor for the description of the present nature of the cyber domain.

There are differences, of course. While Wallace was clearly placing himself in the role of the older fish, dispensing some life guidance to the “young fish” graduating from college that day, when it comes to the understanding of cyberspace, the traditional roles are all too often reversed. For example, not so long ago, Ted Stevens, a venerable politician presiding over the US Senate committee responsible for the regulation of the internet at the time, provided some unintended

* Senior Lecturer in Law, University of Exeter. E-mail: k.macak@exeter.ac.uk. This article was originally presented as a lecture at the Defence Academy of the United Kingdom on 10 December 2018. The present text has been footnoted and lightly edited for clarity. All online resources were last accessed on 28 January 2019. I am grateful to Ana Beduschi, Russell Buchan, Mike Schmitt, and Noam Zamir for their comments on an earlier draft of the article. I also thank Jana Šikorská for her research assistance.

¹ David Foster Wallace, ‘Democracy, English, and the Wars over Usage’ *Harper’s Magazine* (New York, April 2001).

² David Foster Wallace, *This Is Water: Some Thoughts, Delivered on a Significant Occasion, about Living a Compassionate Life* (Hachette 2009).

³ *ibid* 5–6.

⁴ *ibid* 10.

comedy material by publicly describing the internet as “a series of tubes [that] can be filled [by] enormous amounts of material”.⁵ By contrast, today’s “cyber heroes” are often young enough to get ID-ed at the supermarket when they go buy a case of beer. Consider, for instance, the *WannaCry* malware that forced dozens of NHS hospitals to shut down their IT systems last year.⁶ The guy who managed to stop the attack was one Marcus Hutchins, a self-taught hacker who lived with his parents in a small town not too far from Exeter. Mr Hutchins accidentally discovered a kill switch in the malware and stopped it from spreading further.⁷ At the time, he was only 23 years old.

So it may well be that some of the youngest fish intuitively understand the “water” that we are all swimming in much better than many of us older ones do. They know that while cyberspace may be invisible to the naked eye, it has a profound impact on the physical world and our lives within it. Therefore, we can no longer ignore the implications of this new environment. To return to Wallace’s metaphor one more time, we might say that by today, *cyber has become to us what water has always been to fish*.

However, for now there are very few domain-specific rules of behaviour that would apply to this new sphere of human activity. This is true, to a varying extent, for many areas of law that have things to say for human conduct in cyberspace, from domestic criminal law to intellectual property law to human rights law to general international law. And the fact of the matter is that the rules that do exist were developed by people who resemble Senator Stevens much more than they do Mr Hutchins.

Accordingly, adapting the existing legal framework to new situations poses difficult challenges. In this lecture, I am going to explore 1 + 3 such challenges, all of which relate to international humanitarian law (IHL). I have intentionally said “1 + 3”, because in all honesty I believe only the latter three to be true challenges. Those three all relate to “how” questions, in other words, how does the existing law apply to specific novel situations that arise due to the development and exploitation of cyberspace. The first one, by contrast, is a “whether” question, because it considers the baseline issue whether IHL as such applies to cyber operations at all. It follows that before we may proceed to the “how” questions, we must resolve, as a preliminary matter, their “whether” sister.

Whether: Does IHL apply to cyber operations?

It turns out there is some scepticism out there in relation to the “whether” question, including from very prominent places. In 2015, Barack Obama famously described cyberspace as “the wild, wild West”,⁸ which has been interpreted to mean that the cyber world “operated with almost no

⁵ Cory Doctorow, ‘Sen. Steven’s hilariously awful explanation of the Internet’ (*Bingboing*, 2 July 2006) <<https://boingboing.net/2006/07/02/sen-stevens-hilarious.html>>.

⁶ Nicole Perlroth and David E Sanger ‘Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool’ (*The New York Times*, 12 May 2017) <<https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html>>.

⁷ MalwareTech, ‘How to Accidentally Stop a Global Cyber Attacks’ [sic] (*Malwaretech*, 13 May 2017) <<https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html>>.

⁸ Barack Obama, ‘Remarks by the President at the Cybersecurity and Consumer Protection Summit’ (Stanford University, 13 February 2015) <<https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>>.

internationally accepted rules of behavior”.⁹ But that interpretation is simply incorrect. In fact, representatives of the most cyber-active States—including the United States, China, Russia, and many others—who were all participating in a UN-mandated Group of Governmental Experts, have expressly agreed by consensus that international law applies in cyberspace.¹⁰ One would think that because IHL is a part of international law, surely we can say, *a maiori ad minus* if you will, that if the whole applies, then its part must do as well, and end the matter there. IHL applies in cyberspace. But things are unfortunately not that simple.

In the summer of 2017, the same (although slightly differently composed) Group of Governmental Experts failed to reach a consensus on a further set of issues that mostly pertained to “how” questions like those that I will get to in a moment.¹¹ Although no official reasons for the breakdown of that process were ever published, we know that for some participants, the stumbling blocks have included the specific question of applicability of IHL to cyber operations.¹² The likely objectors have included China and Russia, but it fell to Cuba to articulate the crux of the objection. Its representative stated that Cuba could not accept the affirmation of applicability of IHL, because “it would legitimize [a] scenario of war and military actions in the context of [cyberspace]”.¹³

Because this argument reappears with some frequency, it is worth addressing it head-on. To put it as simply as possible, my response is that *regulation does not imply justification*. Just because we acknowledge that the law governs a certain type of conduct, this does not mean that we legitimize that conduct in any way. Actually, it is rather the reverse: IHL imposes restrictions, which serve to constrain the behaviour of belligerents in time of armed conflict.¹⁴ In any event, the question of legality or legitimacy of a particular conflict is one on which IHL is agnostic. This is an issue of the *jus ad bellum* or perhaps of international politics and, as such, it falls strictly outside of the remit of IHL, which is also expressly recognized in the preamble to Additional Protocol I to the Geneva

⁹ David E Sanger, *The Perfect Weapon* (Scribe Publications 2018) 60.

¹⁰ The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ‘GGE Report 2013’ (24 June 2013) A/68/98, 8 para 19.

¹¹ Owen Bowcott, ‘Dispute along cold war lines led to collapse of UN cyberwarfare talks’ (*The Guardian*, 23 August 2017) <<https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges>>.

¹² Michael N Schmitt and Liis Vihul, ‘International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms’ (*Just Security*, 30 June 2017) <<https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>>.

¹³ Cuba’s Representative Office Abroad, ‘71 UNGA: Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security’ (*Representaciones Diplomáticas De Cuba En El Exterior*, 23 June 2017) <<http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>>.

¹⁴ cf ICRC, ‘International Humanitarian Law and the Challenges of Contemporary Armed Conflicts’ (October 2015), 40 (“[A]sserting that IHL applies to cyber warfare is not an encouragement to militarize cyberspace and should not, in any way, be understood as legitimizing cyber warfare.”) <<https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf>>; Gabor Rona ‘Challenges New Weapons and Humanitarian Assistance Present for International Law’ (20 November 2015) (“[S]ome states have asserted that accepting application of IHL legitimizes cyber warfare. Of course, their argument is no more valid than is the false claim that the Geneva Conventions (to which all States are party) legitimizes warfare.”) <<https://www.justsecurity.org/27789/challenges-weapons-humanitarian-assistance-present-ihl/>>.

Conventions.¹⁵ For all these reasons, the Cuban argument must be strongly rejected. IHL does indeed apply in cyberspace.

Having addressed the “whether” question, I am now going to turn to three specific “how” questions. In other words, if you accept that IHL applies to cyber operations, the next question is “how” precisely it applies. There are many issues that one could discuss in this regard. I want to highlight three, and tackle them in a chronological order. I will thus look at one issue that arises before any armed conflict takes place; one that occurs at the very beginning of an armed conflict; and one that is central to the application of the law during an armed conflict. In selecting these particular topics, I am building on an ongoing research project which I lead at the University of Exeter, with the participation of the NATO Co-operative Cyber Defence Centre of Excellence in Tallinn and the National Cyber and Information Security Agency of the Czech Republic.¹⁶ In this project we have asked practitioners to identify issues at the intersection of international law and cyber operations that they considered as particularly problematic in their work. These three were the main ones, which concerned the application of IHL to the conduct in cyberspace.

How #1: How does the weapons review obligation apply to cyber capabilities?

The first challenge relates to one aspect of the application of IHL in peacetime. As you know, the vast majority of IHL obligations only spring into action once an armed conflict is underway. However, there are some important exceptions, which include the duty to respect and ensure respect for IHL,¹⁷ the duty to enact domestic legislation on the protection of the distinctive emblems,¹⁸ or the duty to disseminate IHL in peacetime.¹⁹ Another such rule that applies also in peacetime is Article 36 of Additional Protocol I, which prescribes an obligation for States to conduct a legal review of any new weapon, means or method of warfare.²⁰ It is sometimes said that this obligation reflects customary international law,²¹ but that view is not universally

¹⁵ Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I or AP I) preamble (“the provisions of the Geneva Conventions of 12 August 1949 and of this Protocol must be fully applied in all circumstances to all persons who are protected by those instruments, without any adverse distinction based on the nature or origin of the armed conflict or on the causes espoused by or attributed to the Parties to the conflict”).

¹⁶ University of Exeter, ‘International Cyber Law in Practice: Interactive Toolkit for Legal Advisors and Decision-Makers’ <<https://socialsciences.exeter.ac.uk/law/research/projects/project/?id=614>>.

¹⁷ Common Article 1 to the Geneva Convention of 1949; AP I (n 15) art 1(1); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law* (CUP 2005), r 139 (hereafter *ICRC Study*).

¹⁸ Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GC I) (adopted 12 August 1949, entered into force 21 October 1950) arts 53, 54.

¹⁹ GC I (n 18) art 47; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) art 48; Convention (III) relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) art 127; Convention (IV) relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) art 144; AP I (n 15) art 83; Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978) art 19.

²⁰ AP I (n 15), art 36.

²¹ See, eg, Duncan Blake and Joseph S Imburgia, “Bloodless Weapons”? The need to conduct legal review of certain capabilities and the implications of defining them as “weapons”, (2010) 66 *AFLRev* 157, 163–64; see also William H Boothby, *Weapons and the Law of Armed Conflict* (2nd edn, OUP 2016) 342–43 (“For states that are not party to AP1,

accepted.²² At any rate, even non-parties to the Protocol have to ensure that they do not use weapons that would be unlawful under IHL, even if they are not obliged to conduct a formal review under Article 36. For now, let us focus on the “how” question raised by this provision, which is relevant, at the very least, to all States parties to the Protocol: How does the weapons review obligation apply to cyber capabilities?

Imagine, for example, that a State has developed new sophisticated malware, which is designed to weaken the military capacity of its adversaries in times of armed conflict. The malware replicates itself through the cyber infrastructure and then, after it infects a host system, it tests it for the presence of a particular programmable logic controller (PLC). The state knows that its adversaries use this PLC for the purposes of automated maintenance of military equipment: think robotic repair of military vehicles or aircraft. After infection, one of two things happens. Either the test for the specific PLC is negative; then the malware just conducts one more attempt to spread further through any connected networks before it shuts down for good. Or, if the test is positive, the malware will use a known vulnerability in that PLC in order to *slightly* manipulate the maintenance process. The effect of this manipulation is that the robotic machinery will malfunction and, instead of servicing the equipment, it will physically damage it. Accordingly, the question is how, if at all, we apply the Article 36 obligations to such newly developed cyber capabilities.

To begin with, it is clear that not every cyber capability qualifies as a weapon or a means of warfare under IHL. For example, no State would accept that tools they use for non-destructive exfiltration of data—in other words, for cyber espionage—qualify as means of warfare.²³ As of now, the precise definition of a “cyber weapon” is unsettled in law.²⁴ But it is probably correct to say that the term “weapon” includes at least those cyber means that are capable of conducting attacks as these are defined under IHL, that is, “acts of violence against the adversary”.²⁵ The Harvard Air and Missile Warfare Manual adopted a similar approach²⁶ that was then also incorporated by the Tallinn Manual.²⁷ These rulebooks consider that the essence of a weapon is that it may be used to cause injury, death, damage or destruction. In that sense, it is probably safe

the implied obligation should not necessarily be expressed in the same terms as article 36, but its existence is attested to by the practice of certain states before the adoption of API¹”).

²² Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 465 (rule 110) (hereafter *Tallinn Manual 2.0*); Natalia Jevglevskaja, ‘Weapons Review Obligation under Customary International Law’ (2018) 94 ILS 186, 203–213.

²³ Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, ‘On Cyber Warfare’ (*Chatham House*, November 2010) 8-10 <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf>.

²⁴ See, eg, Gary D Brown and Andrew O Metcalf, ‘Easier Said Than Done: Legal Reviews of Cyber Weapons’ (2014) 7 JNSLP 115, 135 (defining a kinetic and/or a cyber weapon as “an object designed for, and developed or obtained for, the primary purpose of killing, maiming, injuring, damaging or destroying”); *Tallinn Manual 2.0* (n 22), 452 (“cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects”); US, Air Force Instruction 51-401 (3 August 2018), 13 (defining a cyber capability as “any device, computer program or computer script, including any combination of software, firmware or hardware intended to deny, disrupt, degrade, destroy or manipulate adversarial target information, information systems, or networks”).

²⁵ AP I (n 15) art 49.

²⁶ Program on Humanitarian Policy and Conflict Research, ‘Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare’ (Harvard University, 2009), commentary to r 1(t), para. 1.

²⁷ *Tallinn Manual 2.0* (n 22) 451–452 (rule 103, para. 2).

to infer that a malware that causes robotic maintenance machinery to malfunction and thus causes physical damage would qualify as a weapon under IHL.

If this malware is a weapon, then the obligation to conduct a legal review under Article 36 attaches. This review consists of two main steps.²⁸ In the first step, the State must consider whether the weapon in question violates any express specific prohibition on its use. Some weapons are subject to such prohibitions: for example, any new chemical or biological weapon would be covered by the general ban on these types of weapons, prescribed by the relevant international treaties.²⁹ However, for now there are no such prohibitions related to cyber weapons—although this may well change in the future. From time to time, proposals appear that States should enter into so-called “cyber arms control treaties” or agree on specific limitations on the development and use of cyber offensive capabilities.³⁰ If these came to pass and were formulated as binding prohibitions, they would then prevent States from using any capabilities that would fall under the remit of such rules.

Given that there are no means-specific prohibitions that would apply to cyber weapons, the second step is to consider whether the use of the cyber weapon in question is restricted by any of the generally applicable rules of IHL. These rules include, in particular, the prohibition of means of warfare that are of a nature to cause superfluous injury or unnecessary suffering³¹ and the prohibition of means of warfare that are by nature indiscriminate.³² The reference to the “nature” of the means in question in these rules is quite important and it actually takes a lot of the bite out of the weapons review obligation. This is because as long as the weapon under review can potentially be employed in a lawful way, it cannot be said to violate these rules by its nature, and thus the weapon would pass the legal test.³³

So what does all of that mean for a cyber capability like the bespoke malware mentioned earlier? Given that there is no indication that the use of this malware would cause any injury to persons, we may rule out the provisions on superfluous injury or unnecessary suffering. However, this is not the case with respect to the prohibition of inherently indiscriminate means of warfare. Of course, the malware might be specifically designed to target the PLCs, which control *military* equipment. Yet, in order to strike against its target, the malware needs to reach it first. This will

²⁸ See generally ICRC, ‘A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977’ (2006) 88 *International Review of the Red Cross* 931, 938–39 (hereafter ICRC Guide).

²⁹ See Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (signed 10 April 1972, entered into force 26 March 1975) 1015 UNTS 163, art 1; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (signed 13 January 1993, entered into force 29 April 1997) 32 ILM 800, art 1.

³⁰ See, eg, Mette Eilstrup-Sangiovanni, ‘Why the World Needs an International Cyberwar Convention’ (2018) 8 *Philosophy & Technology* 379; Joseph S Nye Jr., ‘The world needs new norms on cyberwarfare’ (*The Washington Post*, 1 October 2015) <https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.fd8262b1bd0c>.

³¹ Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) art 23(e); AP I (n 15) art 35(2); *ICRC Study* (n 17) r 70; *Tallinn Manual 2.0* (n 22) 453–55.

³² AP I (n 15) Art 51(4)(b); *ICRC Study* (n 17), rr 12 and 71; *Tallinn Manual 2.0* (n 22) 455–57; see also Department of Defense of the United States of America, *Law of War Manual* (2016), para. 16.6 (“a legal review of the acquisition or procurement of a weapon that employs cyber capabilities likely would assess whether the weapon is inherently indiscriminate”).

³³ ICRC Guide (n 28) 943.

normally be done by allowing the malicious code to spread through networks. Some of these will be of military nature, others will not. So, the malware will likely have to pass through civilian cyber infrastructure and can thus be expected to have some effect on the proper functioning of that infrastructure.

The lawfulness of such a cyber weapon will thus depend on the extent of this effect if the weapon was used in a normal way, as anticipated at the time of the evaluation.³⁴ So the State must ask itself: Would the malware, once released, spread without any further control of the attacker and could it thus cause reverberating harmful effects without distinction between civilian objects and military objectives? If so, it would fail the test and qualify as an inherently indiscriminate weapon. Accordingly, that would mean the State in question would need to go back to the drawing board.

However, suppose that the planned harmful effects to any civilian infrastructure are temporary and do not exceed mere inconvenience or annoyance. This means that the normal and expected use of the weapon would not reach the level of attack against a civilian object,³⁵ and thus it would not be of a nature to strike military objectives and civilian objects without distinction.³⁶ Suppose further that the acting State is also smart enough to include a “kill switch” in the malware that can immediately stop it from spreading further—like the one that Marcus Hutchins discovered in *WannaCry*. Such a kill switch ensures that the attacker is capable of limiting the effects of the malware if the need arises—for example, if the malware starts spreading in a way that was not anticipated by its authors. Taken together, these safeguards would likely suffice for the weapon to pass the Article 36 review.

How #2: How do the rules on conflict qualification apply to cyber operations?

The second challenge I want to look at sits at the point where the peacetime and wartime legal regimes meet. It is also a “how” question. It asks how the rules on conflict qualification under IHL apply to cyber operations. In other words, is it possible for a cyber operation to trigger an armed conflict and, in doing so, activate the applicability of IHL?

Note that this question is separate from the question how IHL applies to cyber operations once an armed conflict is under way. I will look at one aspect of that question in the last part of this lecture. For now, I am focussing only on the threshold point: can a cyber operation start an armed conflict just like the launch of a kinetic missile or an exchange of mortar fire between two belligerents?

³⁴ Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross 1987) (ICRC APs Commentary) 423 para 1466.

³⁵ See also Michael N Schmitt, ‘Wired Warfare: Computer Network Attack and *Jus in Bello*’ (2002) 84 International Review of the Red Cross 365, 377 (arguing that “inconvenience, harassment or mere diminishment in quality of life” does not qualify as a violent consequence that would bring the original act within the ambit of “attack” under IHL).

³⁶ Cf. *Tallinn Manual 2.0* (n 22) 457 (commentary to rule 105, para. 5: “the uncontrollable spread of harmless effects or those that are merely inconvenient or annoying is irrelevant when assessing the legality of a means or method of cyber warfare”).

I should also note that there is no generic notion of “armed conflict” under IHL.³⁷ Instead, IHL distinguishes between an international armed conflict (IAC) and a non-international armed conflict (NIAC), while the existence of each is subject to different legal tests. This is not the place to explore these tests in detail.³⁸ However, it can be summarized that the legal threshold is set lower for IACs than it is for NIACs. Whereas for a NIAC to come about, the situation must meet the twin requirements of organization and intensity, IACs are subject to a lower bar. As the ICTY held in the *Tadić* case in 1995, an IAC starts whenever there is any resort to armed force between States.³⁹ Because this threshold is less demanding than that required for NIACs and because our time today is limited, let us look at whether and when this lower line can be crossed by a cyber operation.

As I said earlier, cyberspace is to a large extent an invisible reality that surrounds us all. As such, there are many, many cyber operations that occur at all times everywhere in the world. To say that 99.99% of them do not come close to a “resort to armed force” would still be a massive understatement. Even those operations that have been attributed to States by other States and labelled as violations of international law have not been described as a use of force. For a recent example, consider the statement issued by the UK National Cyber Security Centre in October this year. The NCSC accused the Russian military intelligence service of “reckless cyber attacks”, which have been conducted “in flagrant violation of international law”.⁴⁰ Some of these have caused considerable disruption around the world: confidential files were stolen and leaked, e-mail accounts of journalists and diplomats were hacked, IT infrastructure was made inoperable, and so on. But despite the strongly worded statement, the UK did not suggest that any of those operations had qualified as a use of force or armed force.⁴¹ This is the case with all—I repeat, all—cyber operations conducted thus far. We are yet to see a State accusing another State of having started an international armed conflict through cyber means. Therefore, while the importance of this question is obvious, we should remember that for now it is a hypothetical one.

What most experts agree on is that if the effects of cyber operations are equivalent to classic kinetic military operations, then the resulting situation would amount to an international armed conflict.⁴² Imagine, for example, that a cyber operation against a State succeeds in bringing down the air traffic control system of that State or in opening the floodgates of dams on that State’s territory. As a result, many people die and significant material damage occurs. Provided that the

³⁷ See Dino Kritsiotis, ‘The Tremors of Tadić’ (2010) 43 *Isr L Rev* 262, 293–99; Marko Milanovic, ‘The Applicability of the Conventions to “Transnational” and “Mixed” Conflicts’ in Andrew Clapham, Paola Gaeta, and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015) 30 paras 8–10; Kubo Mačák, *Internationalized Armed Conflicts in International Law* (OUP 2018) 19–20.

³⁸ See, eg, Mačák (n 37) 14–21.

³⁹ ICTY, *Prosecutor v Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-AR72, Appeals Chamber II, 2 October 1995, para 70.

⁴⁰ National Cyber Security Centre, ‘Reckless campaign of cyber attacks by Russian military intelligence service exposed’ (4 October 2018) <<https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>>.

⁴¹ For further discussion of this incident and its implications for international cyber law, see Kubo Mačák, ‘On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law’ (2019) 113 *American Journal of International Law Unbound* 81, 83–84.

⁴² See, eg, *Tallinn Manual 2.0* (n 22) 375 (rule 80); Tristan Ferraro and Lindsey Cameron, ‘Article 2: Application of the Convention’, in ICRC (ed), *Commentary on the First Geneva Convention* (CUP 2016) 92 para 255; Andrew Clapham, ‘Concept of International Armed Conflict’ in Clapham et al, *Geneva Conventions* (n 37) 22–23.

cyber operation is attributable to another State, it would undoubtedly bring about a situation of an international armed conflict between those two States. Simply put, there is no reason to distinguish between such attacks depending on the means that were used to bring about these effects.

However, beyond these clear-cut cases the law is very much unsettled. Many cyber operations do not and will not bring about effects comparable to kinetic attacks. While they may not cause death or injury or even destruction or damage, they may still result in considerable disruption. For instance, an operation against the power grid—as we saw in Ukraine on at least two occasions since 2015—can result in hundreds of thousands of people losing their access to electricity.⁴³ Of course, Ukraine was already engaged in an ongoing armed conflict when these incidents occurred, so they did not present an opportunity for States to come down one way or another. But such incidents will happen again and it is through future State practice that this uncertainty in the law will be resolved.⁴⁴ Still, there is no doubt that if an armed conflict is under way, the applicable rules of IHL will apply also to cyber operations. The final challenge I want to consider today relates precisely to such situations.

How #3: How do the rules on targeting apply to cyber operations against data?

This is again a “how” challenge in that it examines how the rules of targeting apply to cyber operations. The cornerstone of the law of targeting is in the principle of distinction, according to which the belligerents must at all times distinguish between civilian objects and military objectives and accordingly direct their operations only against military objectives.⁴⁵ As far as objects are concerned, the crucial distinction therefore is between civilian objects and military objectives. In order to distinguish one from the other, IHL has developed a detailed definition of military objectives, which is today enshrined in article 52, para. 2 of Additional Protocol I⁴⁶ and considered to reflect customary international law.⁴⁷ But does this definition apply to operations which do not aim to destroy or damage physical objects, but instead are oriented against data?

In order to give that abstract issue some concrete contours, consider the following example. Imagine that Arcadia and Utopia are two independent States that are engaged in an international armed conflict against one another. At one point, Arcadia decides to conduct a cyber operation against the central registry office of its enemy. The intended target, the Utopian Central Registry Office, is a governmental authority, which maintains digital records on Utopian citizens, with regard to all non-military purposes such as census taking, the provision of social benefits, voting, and taxation. Now let us suppose further that Arcadia is successful and its operation results in the destruction of all data held by the registry office—but it does not cause any physical destruction, and it equally does not affect the cyber infrastructure which supports the system used by the office.

⁴³ Andy Greenberg, “Crash Override: The Malware that Took Down a Power Grid” (6 December 2017) <<https://www.wired.com/story/crash-override-malware/>>.

⁴⁴ See also Ferraro and Cameron (n 42) 91 para 256.

⁴⁵ AP I (n 15) art 48.

⁴⁶ AP I (n 15) art 52(2) (“Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”).

⁴⁷ ICRC *Study* (n 17), r 8.

In other words, the data is gone, but all the computers seemingly work as they did before. The question therefore is—did Arcadia violate IHL by destroying the datasets held by the Utopian authorities?

Before answering that question, it is useful to stop and pause for a moment. Putting the law aside for a moment, what exactly do we mean by “destruction”? Is it even correct to speak of “destruction of data”? We store data by converting it into many, many binary numbers and then recording them on data drives. The process of recording these numbers actually means magnetizing tiny areas of a hard disk either north or south – or, in more modern drives, charging or not charging a series of electrical cells. So, if I delete some of the data on your smartphone, I am not destroying any part of your phone, but I am merely changing the way some of its parts were charged before. What does get “destroyed”, or in other words, what ceases to be even though it had been before, is the information that was represented by the previous configuration. It may be of interest to this audience that a prescient report published by the Defence Academy argued already in 2013 that we need to establish “an information-centric definition of ‘destruction’.”⁴⁸ Under such definition, it would be correct to say that what I did was to destroy your data indeed. However, the report in question was by the admission of its own authors a big-picture endeavour focussed on broad implications of the cyber domain for security strategy.⁴⁹ So what does the *existing* law of armed conflict have to say about such operations?

The answer to that question turns on the “how” question, that is, how we apply the definition of military objectives to attacks against data. You will recall that the applicable definition in article 52, para. 2 of Additional Protocol I limits itself to “objects”. The relevant part states, “In so far as objects are concerned, military objectives are limited to those objects which,” and the remainder of the definition sets out the conditions that objects must meet in order to be targetable during armed conflicts.⁵⁰ Those that do not so qualify are to be seen as civilian objects and as such they are strictly protected by the law.

There are two main approaches that have emerged thus far. On the one hand, some experts, including the majority of the participants in the Tallinn Manual project, consider the notion “object” to be limited to something with physical properties that is visible and tangible in the real world.⁵¹ This view is based on a textual interpretation of the term “object” and it finds further

⁴⁸ Hardin Tibbs (ed), *The Global Cyber Game* (The Defence Academy of the United Kingdom, 2013), 37 <<http://www.futurelens.com/wp-content/uploads/2014/04/The-Global-Cyber-Game.pdf>> (“The key to understanding this zone of the gameboard is establishing an information-centric definition of ‘destruction’. The usual meaning is physical destruction, and this is the sense used in international law for the definition of ‘use of force’, which is taken to involve serious physically destructive and lethal acts.”).

⁴⁹ *ibid*, ii (“The Inquiry’s overall remit was first to consider the broad question ‘how should the cyber domain be conceptualized?’ and in the light of that to examine the *implications for security strategy generally*, the issues raised for state actors in the Internet age, new power relationships, possible sources and modes of future conflict, and the steps that need to be taken to prepare for a range of plausible possibilities. This report gives an overview of the Cyber Inquiry’s *big-picture conclusions*.”).

⁵⁰ AP I (n 15) art 52(2).

⁵¹ *Tallinn Manual 2.0* (n 22), commentary to rule 100, para. 5–6 (noting that the majority of experts considered that due to it being intangible, data does not fall within the ordinary meaning of the term object, which is “something visible and tangible”) (internal quotation marks deleted); but see Michael N Schmitt, “The Notion of ‘Objects’ during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision” (2015) 48 *IsrLR* 81, 93 (noting that although the “visible and tangible” criterion influenced the Tallinn Manual experts’ deliberations, it was not dispositive).

support in the ICRC commentary to the Additional Protocols.⁵² On this view, cyber operations against data do not fall within the ambit of IHL unless the operation in question causes some physical effect or at least a loss of functionality of the target system.⁵³ In the Arcadian-Utopian example, this would mean that the operation against the registry office would not violate IHL even though it would be obviously tremendously disruptive to civilian life in Utopia.

On the other hand, others, including myself, hold the view that data falls within the notion of “object” under IHL.⁵⁴ I would expect that this view may find some favour among those in the audience today who agree with the “information-centric” approach proposed by the Defence Academy report I mentioned earlier.⁵⁵ To my mind, it also follows quite clearly from the correct application of the rules on treaty interpretation under international law.⁵⁶ This is for the following reasons.

First, whatever the ordinary meaning of the term “object” was in 1977, today it should be seen as covering information stored in computer systems and devices—just ask any teenager if they would consider it as a loss of something of value if you were to wipe out the entire contents of their Instagram account. Second, this is confirmed also by examining the context of article 52, para. 2. Across the entire relevant section of the Protocol, the term “object” is used as something susceptible to destruction, capture or neutralization. It thus does not matter that data is not visible or tangible in the same way that a bridge is. What matters is that both may be attacked by the adversary with the result that what had been there before will be significantly altered or absent altogether: i.e., damaged or destroyed. Third, the inclusive view is also in line with the object and purpose of the Protocol, which is the protection of victims of armed conflicts. Civilians are obviously one of the categories of such victims and because this view brings civilian datasets within the framework of IHL, it thus also fosters the relevant object and purpose.⁵⁷

Under the inclusive view, the cyber operation against the Utopian datasets would have to be justified against the definition of military objectives. Because civilian data on voting or taxation do not contribute to military action and because their destruction does not offer any definite military advantage, the operation would thus have to be seen as a violation of IHL. I think this is the correct conclusion, but the debate is certainly still going on.⁵⁸

⁵² *Tallinn Manual 2.0* (n 22), commentary to rule 100, para. 5 (“An ‘object’ is characterised in the ICRC Additional Protocols 1987 Commentary as something ‘visible and tangible.’”); *ICRC APs Commentary* (n 34) 633–34 paras 2007–08.

⁵³ *Tallinn Manual 2.0* (n 22), commentary to rule 100, para. 6.

⁵⁴ Heather A Harrison Dinniss, ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ (2015) 48 *IsrLR* 39, 44; Kubo Mačák, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ (2015) 48 *IsrLR* 55, 67–68.

⁵⁵ Tibbs (n 48) 37.

⁵⁶ Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331, arts 31–32.

⁵⁷ See further Mačák (n 54) 77–80.

⁵⁸ See, eg, Tim McCormack, ‘International Humanitarian Law and the Targeting of Data’ (2018) 94 *ILS* 222; Robert McLaughlin, ‘Data as a Military Objective’ (*Australian Institute of International Affairs*, 20 September 2018) <<http://www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/>>; Michael N Schmitt, ‘Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations’ (2019) __ *International Review of the Red Cross* __ (forthcoming).

Conclusions

So, in conclusion, I would like to say this. Many years before smartphones were invented, John Perry Barlow—a cyber activist if there ever was one—defined cyberspace in the following way: “Cyberspace is where you are when you’re on the phone.”⁵⁹ Under that definition, if you look around the room right now, you may discover that some of us are in cyberspace even at this very moment. But my claim today has been that we are in cyberspace even when we are not actually scrolling through our Facebook feeds. The physical world of flesh and blood that we all inhabit has now become too intertwined with the cyber domain for the two to ever be fully separate again. This presents many opportunities, but also some prominent challenges. I would thus like to close by complimenting the Defence Academy for its foresight and willingness to offer a platform to discuss some of these challenges today. It is an area in which the law is evolving and will continue doing so. And it is only through discussion and engagement that we will come closer to understanding and influencing the trajectory of this development.

Thank you.

⁵⁹ JP Zaleski, *The Soul of Cyberspace: How New Technology is Changing Our Spiritual Lives* (HarperEdge 1997) 29.